AMENDMENTS IN THE CLAIMS

1. (currently amended) A method for providing access protection to electronic storage devices, said method comprising the steps of:

providing a device-stored hardware-level security code for a storage device on which is stored an electronic file to which user access is restricted ~~access is desired~~;

initializing said security code within said storage device during set-up of said storage device, wherein said security code is unique to said storage device and is required to complete all accesses to said storage device, including read accesses and write accesses;

providing within an operating system (OS) of a user computer an OS-extension that enables (1) retrieval of said security code from said storage device to said user computer system and (2) blocking access to said storage device by processes on said user computer system when a user-provided code does not match the security code retrieved from the storage device;

wherein the OS-extension enables use of the hardware-level security code within a localized, OS-level security checking process, wherein said hardware-level security code is loaded into the OS-level security checking process whenever a user process on the user computer system attempts a read or write operation on said storage device; and

allowing access by said user process to said storage device from the user-computer system with the OS-extension only when ~~a~~ the user-provided code is determined by the localized, OS-level security checking process to ~~enters a user code that~~ matches said hardware-level security code.

2. (currently amended) The method of Claim 1, wherein said initializing further ~~comprising the steps of initializing said security code within a microcode of said storage device, wherein~~ comprises:

blocking access to said storage device ~~is denied~~ during said initializing ~~step~~;

placing said security code within pre-determined bits of a microcode of the storage device, wherein said predetermined bits are defaulted to a default value when no security code is placed therein.

3. Canceled

4. (currently amended) The method of Claim ~~3~~ 1, wherein said ~~defining step includes:~~ ~~adding a hardware security code checking process to an OS operation for supporting a security code comparison with a user access code when a user requests a read and write on said~~ storage device is one of multiple storage devices accessible via the OS and each of said multiple storage devices is configurable with a unique security code, said method further comprising:

determining to which one of said multiple storage devices access is being requested; and

comparing the user-entered code against the particular security code associated with that one storage device, wherein access granted/denied to a first one of the multiple storage devices is independent of access granted/denied to a second one of said multiple storage devices, wherein further the security code of the first device is unique among security codes of the multiple available storage devices.

5. (currently amended) The method of Claim [[4]] 1, further comprising the step of:

receiving at the OS-level a process request for access to said storage device;

retrieving from the storage device the security code stored within microcode of the device and forwarding the security code to the localized, OS-level security checking process;

evaluating ~~via said hardware security code checking process~~ said security code ~~returned~~ retrieved for a pre-defined default value ~~by said file protocol~~; and

in response to said security code having a ~~pre-determined~~ pre-defined default value, providing said user with unrestricted access to said storage device.

6. (currently amended) The method of Claim 5, wherein, when said security code does not have said pre-defined default value, said method further ~~comprising the step of~~ comprises:

comparing said security code with said user provided access code ~~when said authentication code is not said pre-determined default value~~;

providing access when said security code matches said user-provided access code; and

denying access when said security code does not match said user-provided access code.

7. (currently amended) The method of Claim 5, further comprising: ~~the step of outputting an access deny message of said user~~

providing process-based security checks for access to said storage device, wherein an access security check is initiated for each read/write access to said storage device by a different process executing on said local user computer system; and

wherein each process associated with a single application initiated by the user is provided a same user-entered access code as a default and individual processes may be provided a hardware-specific access code for the particular storage device to which the process requests access.

8. (currently amended) The method of Claim 7, further comprising the steps of:

restricting a subsequent request for access to said storage device by a user when said security code does not match said user access code during an initial comparison of the codes ~~request by said user~~; and

when the codes do not match, automatically terminating at least the process requesting access that was ~~a job~~ submitted by said user.

---

9. (currently amended) A computer program product comprising:

a computer readable medium; and

program instructions stored on said computer readable medium for implementing file access protection by:

~~providing~~ retrieving a locally-stored hardware-level security code for a ~~drive~~ remote storage device on which is stored an electronic file to which ~~restricted~~ user access is restricted ~~desired~~, wherein said security code is placed within said storage device during set-up of said storage device, wherein said security code is unique to said remote storage device and is required to complete all accesses to said storage device, including read accesses and write accesses;

providing within an operating system (OS) of a user computer an OS-extension that enables (1) retrieval of said security code from said storage device to said user computer system and (2) blocking access to said storage device by processes on said user computer system when a user-provided code does not match the security code retrieved from the storage device;

wherein the OS-extension enables use of the hardware-level security code within a localized, OS-level security checking process, wherein said hardware-level security code is

loaded into the OS-level security checking process whenever a user process on the user computer system attempts a read or write operation on said remote storage device; and

allowing access to said storage device only when a the user-provided code is determined by the local, OS-level security checking process to ~~enters a user code that~~ matches said hardware-level security code ~~is provided.~~

10. (original) The computer program product of Claim 9, further comprising program instructions for initializing said security code within a microcode of said drive, wherein access to said drive is denied during said initializing step.

11. Canceled

12. (currently amended) The computer program product of Claim ~~11~~ 9, wherein storage device is one of multiple storage devices accessible via the OS and each of said multiple storage devices is configurable with a unique security code, said program product further comprising program instructions for:

~~adding a hardware security code checking process to an OS operation for supporting a security code comparison with a user access code when a user requests a read and write with respect to said storage device.~~

determining to which one of said multiple storage devices access is being requested; and

comparing the user-entered code against the particular security code associated with that one storage device, wherein access granted/denied to a first one of the multiple storage devices is independent of access granted/denied to a second one of said multiple storage devices, wherein further the security code of the first device is unique among security codes of the multiple available storage devices.

13. (currently amended) The computer program product of Claim 12, further comprising program instructions for:

receiving at the OS-level a process request for access to said storage device;

retrieving from the storage device the security code stored within microcode of the device and forwarding the security code to the localized, OS-level security checking process;

~~evaluating via said hardware security code checking process~~ said security code ~~returned~~ retrieved for a pre-defined default value ~~by said file protocol~~; and

in response to said security code having a ~~pre-determined~~ pre-defined default value, providing said user with unrestricted access to said storage device.

14. (currently amended) The computer program product of Claim 13, wherein, when said security code does not have said pre-defined default value, said program product further ~~comprising~~ comprises program instructions for:

comparing said security code with said user-provided code ~~when said security code is not said pre-determined default value~~;

providing access when said security code matches said user-provided access code; and

denying access when said security code does not match said user-provided access code.

15. (currently amended) The computer program product of Claim 13, further comprising program instructions for:

~~outputting an access denied message of said user, and canceling the job submitted by said user.~~

providing process-based security checks for access to said storage device, wherein an access security check is initiated for each read/write access to said storage device by a different process executing on said local user computer system; and

wherein each process associated with a single application initiated by the user is provided a same user-entered access code as a default and individual processes may be provided a hardware-specific access code for the particular storage device to which the process requests access.

16. (currently amended) The computer program product of Claim 15, further comprising program instructions for:

restricting a subsequent request for access to said storage device by a user when said security code does not match said user access code during an initial comparison of the codes ~~request by said user~~; and

when the codes do not match, automatically terminating at least the process requesting access that was submitted by said user.

17. (currently amended) A data processing system comprising:

a processor;

a memory linked to said processor via an interconnect;

an input/output (I/O) device;

a drive on which is stored one or more files for which user-access is restricted ~~access is desired~~, said drive also having a hardware-level security code stored thereon and retrievable by a predefined OS-process; and

an OS executing on said processor that provides support for assigning a hardware-level security code for said drive and includes code for implementing the predefined OS-process that enables ~~allows~~ user access to said file ~~by user~~ only when a user-provided ~~entered~~ access code matches said security code, which is retrieved by said OS in response to a request to access said drive.

18. (currently amended) The data processing system of Claim 17, wherein further said OS includes an OS extension by which an assigning of said security code and access to said drive are implemented.

19. (currently amended) The data processing system of Claim 18, wherein further said OS extension includes program instructions for:

adding a remote hardware security code checking ~~code~~ process to an OS support of user-initiated processes on the data processing system, wherein said security code checking process ~~operation for supporting~~ provides a security code comparison with a the user-provided ~~access~~ code when a the user requests a read and write on said drive; and

identifying specific locations on flash ROM or EEPROM on said drive that ~~houses~~ maintains drive microcode ~~on said drive for~~ and initializing said security code within said drive microcode.

20. (currently amended) The data processing system of Claim 18, wherein further said OS extension includes program instructions for:

evaluating via said hardware security code checking process said security code returned by ~~said file protocol~~; and

in response to said security code having a pre-determined default value, providing said user with unrestricted access to said drive.

21. (currently amended) The data processing system of Claim 20, wherein further said OS extension ~~processes~~ includes program instructions for comparing said ~~authentication~~ security code with said user-provided ~~entered access~~ code when said ~~authentication~~ security code is not said pre-determined default value.

22. (currently amended) The data processing system of Claim 21, wherein further said OS extension further includes program instructions for outputting an access deny message to said user when said security code does not match said access code.

23. (original) The data processing system of Claim 21, further comprising means for restricting a subsequent request for access to said storage device by a user when said security code does not match said user access code during an initial request by said user.

24. (currently amended) A storage system comprising:

a connectable communication medium for connecting to a local computer implementing software-based operating system (OS) and user processes;

a recordable medium for recording data;

at least one piece of data that is accessible from a user computer that is connected to said storage system, wherein said at least one piece of data is not general access data; ~~and~~

a security code, stored on said storage system, that is unique to said storage system and which must be matched against a user-provided code to enable user access from the user computer to the at least one piece of data stored on the recordable medium, wherein said security code protects said data recorded on said recordable medium from unauthorized access;

means for receiving a request for access to said at least one piece of data on said storage medium; and

means for automatically issuing said security code to a requesting operating system extension in response to receipt of said request.

25. Canceled

26. Canceled

28. (New) The method of Claim 8, wherein when the process is a part of a larger job containing multiple processes, said method automatically terminates said job when said codes do not match.

29. (New) The computer program product of Claim 16, wherein when the process is a part of a larger job containing multiple processes, said program instruction includes program instructions for automatically terminating said job when said codes do not match.